

CLAIMS

1. A data processing method providing first authentication use data used for authentication by means to be authenticated to the means to be authenticated when authenticating means holding key data uses the key data designated by the means to be authenticated holding the first authentication use data for encryption to generate second authentication use data, uses the second authentication use data to authenticate with the means to be authenticated, and performs processing related to the key data conditional on confirming that the first authentication use data and the second authentication use data are the same due to the authentication, comprising:

a first step of generating the first authentication use data by using the key data related to the processing permitted to the means to be authenticated among processing relating to the authenticating means and performing the encryption, and

a second step of providing the first authentication use data generated in the first step and key designation data designating the key data used in the first step to the means to be authenticated.

2. A data processing method as set forth in claim 1, wherein the second step comprises a step of

writing the first authentication use data and the key designation data in an integrated circuit used by the means to be authenticated.

3. A data processing method as set forth in
5 claim 1, wherein the first step comprises a step of generating the first authentication use data by using the key data related to function of the authenticating means permitted by the means to be authenticated or an access to data held by the authenticating means.

10 4. A data processing method as set forth in claim 1, wherein

the first step comprises of a step of generating the first authentication use data by encrypting authentication use data generated by using
15 first key data related to the processing permitted to the means to be authenticated by a first user, by using second key data related to the processing permitted to the means to be authenticated by a second user received authority by the first user, and

20 the second step comprises a step of providing the key designation data designating the second key data further to the means to be authenticated.

5. A data processing method as set forth in claim 4, wherein the first step comprises a step of using

first tamper-proofing key data managed by the first user further to encrypt authentication use data generated by using the first key data, encrypting authentication use data generated by the encryption by using the second key data, and encrypting authentication use data obtained by the encryption using the second key data by using second tamper-proofing key data distributed to the second user by the first user to generate the first authentication use data.

10 6. A data processing method as set forth in claim 1, wherein the first step comprises a step of generating the first authentication use data by using a plurality of the key data related to a plurality of processing relating to the authenticating means
15 respectively.

 7. A data processing method as set forth in claim 6, wherein the first step comprises a step of generating the first authentication use data by using the key data related to a plurality of processing including
20 the function of the authenticating means and the access to data held by the authenticating means respectively.

 8. A data processing method as set forth in claim 3, wherein the first authentication use data is generated by using the single key data related to an

access to a plurality of data module when the authenticating means holds a plurality of the data module as the data.

9. A data processing method as set forth in
5 claim 1 further comprising:

a third step by which the means to be authenticated provides the key designation data to the authenticating means,

a fourth step by which the authenticating
10 means generates the second authentication use data with the predetermined generation method by using the key data designated by the key designation data received in the third step,

a fifth step by which the means to be
15 authenticated uses the first authentication use data and the authenticating means uses the second authentication use data generated in the fourth step, authentication is performed, and

a sixth step by which the authenticating
20 means executes processing related to the key data in response to an indication from the means to be authenticated when the authenticating means judges that the first authentication use data and the second authentication use data are the same by the

authentication in the fifth step.

10. A data processing method as set forth in claim 1, wherein the first step comprises a step of generating the first authentication use data by using the
5 key data to encrypt predetermined data.

11. A data processing method as set forth in claim 1,

further comprising a third step of specifying the key data corresponding to a service designated by the means to be authenticated based on correspondence data of
10 the service that is a use target of the means to be authenticated and single or a plurality of the key data related to processing relating to the authenticating means corresponding to the service, wherein

15 the first step comprises a step of generating the first authentication use data by using the key data specified in the third step.

12. A data processing method as set forth in claim 11, wherein the third step comprises a step of
20 providing a screen making the means to be authenticated designate the service.

13. A program executed by a data processing device providing first authentication use data used for authentication by means to be authenticated to the means

to be authenticated when authenticating means holding key data uses the key data designated by the means to be authenticated holding the first authentication use data for encryption to generate second authentication use data, 5 uses the second authentication use data to authenticate with the means to be authenticated, and performs processing related to the key data conditional on confirming that the first authentication use data and the second authentication use data are the same due to the 10 authentication, comprising:

a first step of generating the first authentication use data by using the key data related to the processing permitted to the means to be authenticated among processing relating to the authenticating means for 15 the encryption, and

a second step of providing the first authentication use data generated in the first step and key designation data designating the key data used in the first step to the means to be authenticated.

20 14. A program as set forth in claim 13, wherein the first step comprises a step of generating the first authentication use data by using the key data related to function of the authenticating means permitted by the means to be authenticated or an access to data held by

the authenticating means.

15. A data processing device providing first authentication use data used for authentication by means to be authenticated to the means to be authenticated when authenticating means holding key data uses the key data designated by the means to be authenticated holding the first authentication use data for encryption to generate second authentication use data, uses the second authentication use data to authenticate with the means to be authenticated, and performs processing related to the key data conditional on the authentication confirming that the first authentication use data and the second authentication use data are the same, comprising:

a first means for generating the first authentication use data by using the key data related to the processing permitted to the means to be authenticated among processing relating to the authenticating means for the encryption, and

a second means for providing the first authentication use data generated in the first means and key designation data designating the key data used in the first means to the means to be authenticated.